

Une semaine avec les policiers de la CyberCrim' (1/2)

«Morbac 1»

Q va à Séoul

Avec eux, disques durs, fichiers informatiques ou pistes magnétiques de cartes bancaires ne gardent pas longtemps leurs secrets. Trente-cinq flics chevronnés lorgnent les piratages ou prêtent leur assistance experte dans d'autres enquêtes.

Qui veut aller en Corée? Toi, tu parles anglais, ça ne te tente pas? Allez, qui veut aller passer une semaine en Corée? Ce matin, le commandant Philippe (1) donne de la voix parmi ses troupes de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). L'imprononçable OCLCTIC est engagé sur tous les fronts de cette «forme de criminalité nouvelle et en constante évolution» – dit Dominique de Villepin – qu'est la cybercriminalité. Le commandant Philippe est un peu camelot quand il s'agit de recruter un volontaire pour aller échanger sur la cybercriminalité avec les policiers de Séoul. Une tête apparaît par l'entrebâillement d'une porte: «Moi, je ne peux pas, chef, j'ai mes écouteurs à finir.» Les autres fonctionnaires ont le nez dans leur écran.

C'est à n'y rien comprendre de la police. Quand des gardiens de la paix se morfondent immobiles au fond de leur guérite, les gars de l'OCLCTIC semblent faire la fine bouche pour partir à l'autre bout du monde. «Trop de trucs à faire», dit un enquêteur. «Moi, je ne parle pas assez bien anglais», ajoute un autre. Mais le commandant Philippe est du genre tenace. Il revient à la charge et finit par convaincre Didier, un policier affichant une photographie de disque dur en fond d'écran de son ordinateur. «Faut être tout de même un peu maso», soupire son voisin qui préfère contempler la silhouette de Liv Tyler sur son PC.

128 affaires en 2003

Avant de s'adonner pleinement à sa passion pour Windows et Linux, Didier était gardien de la paix à l'Élysée. Donc plutôt du genre planton. Ça aide pour se réveiller en poulet voyageur. A l'OCLCTIC, il a hérité du surnom «Morbac 1» décerné par le commandant Philippe. Ce qui est un

compliment dans le langage maison. «Quand il s'accroche, il ne lâche pas» martèle l'officier, pas mécontent d'avoir déniché un candidat pour la Corée.

Avec sa barbe et ses Gitanes sans filtre, le commandant Philippe ressemble à un célèbre juge antiterroriste. Dans sa première vie professionnelle, il était professeur certifié de mathématiques dans un lycée de Fougères (Ille-et-Vilaine). Il a gardé de l'enseignement le goût des leçons bavardes et précises au tableau blanc pour décrire les «usines à gaz» que sont les ordinateurs décortiqués par l'OCLCTIC. Les trente-cinq enquêteurs de l'office sont à la cybercriminalité ce que les flics de la crim' sont aux homicides ou les policiers des brigades de répression du banditisme (BRB) aux braqueurs: des flics chevronnés dans leur spécialité. Ni trace de sang, ni empreinte ADN dans leurs enquêtes. Mais des fichiers informatiques, des pistes magnétiques de cartes bancaires, des logiciels piratés. «Ma scène de crime à moi, c'est le disque dur de votre ordinateur», explique le commandant Philippe. On assiste aussi bien les stups que

«Rechercher un mot dans un disque dur, c'est rechercher un mot dans 65 semi-remorques de papier.»

Le commandant Philippe

l'antiterrorisme dans leurs enquêtes. On voit toutes les infractions que l'informatique peut accompagner.»

Il y a vingt ans, l'officier construisait son premier ordinateur personnel avec des cartes achetées place de la République, à Paris. A l'époque, le PC et le Mac étaient encore des intrus dans la police. Au mieux des traitements de texte. Il y a dix ans, le commandant Philippe est entré dans la toute nouvelle Brigade centrale de répression de la criminalité informatique. «C'étaient les balbutiements. Il a fallu tout mettre au point: une stratégie de perquisition sur ordinateur, apprendre à faire des

constatations sans modifier le contenu de la machine.» L'année dernière, l'OCLCTIC a traité 128 affaires mettant en cause 54 personnes.

Le piratage informatique serait une affaire d'hommes, selon la patronne du commandant Philippe: «Ilya quelques femmes dans les dossiers de fraudes aux cartes bancaires, indique Catherine Chambon, commissaire divisionnaire. Mais je n'ai pas vu passer une fille en garde à vue. Des mères éplorées qui viennent nous voir parce que leurs enfants sont trop géniaux, oui.»

On a beau chercher dans les locaux de l'OCLCTIC, les géoles de garde à vue restent introuvables et le commandant Philippe élude le sujet. «C'est vrai que les gens sont un peu surpris quand ils se retrouvent en garde à vue au milieu des ordinateurs, dit un enquêteur. En général, ils ne "chiquent" (2) pas très longtemps. Ils aiment montrer qu'ils savent. Se faire attraper, ça peut faire partie de la reconnaissance.»

Désosseur de disque dur, un métier

Quatre jours et quatre nuits. A trifouiller le contenu de quinze ordinateurs dans l'enquête sur Richard Reid, le terroriste aux baskets piégées. Ça fait partie des riches heures du groupe «Assistance technique-Interceptions» de l'OCLCTIC. Ce sont mes «danseuses» dit Catherine Chambon en désignant ses enquêteurs, véritables désosseurs de disques durs et toujours gourmands en achats de matériel informatique.

Les désosseurs ont été réquisitionnés pour le nouvel an 2002 quand la section antiterroriste de la brigade criminelle a saisi quinze ordinateurs dans l'enquête sur Richard Reid. Ils s'y sont mis à quatre, «nuit et jour», pour analyser les disques durs du cybercafé qu'avait fréquenté le Britannique dans le XVIII^e arrondissement à Paris. «Le cybercafé avait tourné dix jours après le départ de Richard Reid. Ça faisait de l'eau sous les ponts en matière de fichiers supprimés et réécrits sur les

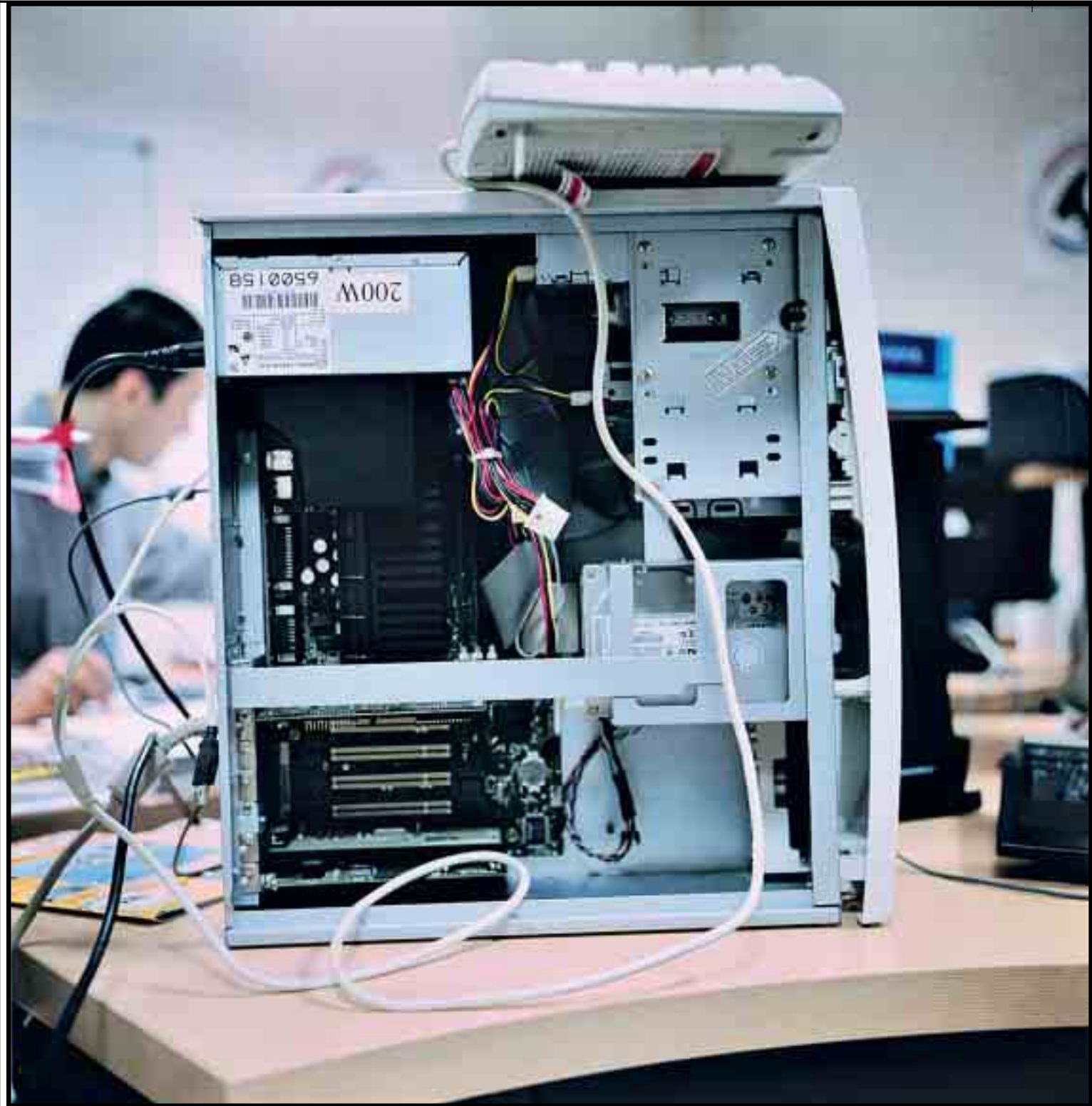
disques durs, raconte un officier. On est partie de l'adresse électronique qu'il avait donnée aux Etats-Unis. On a tiré cette ficelle. Trois, quatre disques durs ont réagi. On a récupéré une cinquantaine de mails "entrants" et "sortants". On a compris que Richard Reid était passé en Belgique auparavant et aussi dans un cybercafé d'Amsterdam.»

Les cyberflics emportent un drôle de paquetage quand ils vont perquisitionner en compagnie de leurs collègues de PJ: le «Sacasa», qui est un gros PC noir (une vingtaine de kilos), caréné comme un 4x4 soviétique. Pour ouvrir les fichiers de l'ordinateur perquisitionné, le «Sacasa» contient plus d'une vingtaine de logiciels différents.

L'un d'eux recherche les fichiers supprimés sur le disque dur. «On regardait si la "bête" est en réseau ou pas afin de vérifier si, à l'autre bout de la France, un gars n'est pas en train de supprimer à distance des fichiers. Après de multiples précautions, on éteint la machine. Quand on entre dans la pièce, plus rien ne doit changer sur l'ordinateur. S'il est éteint, surtout on ne l'allume pas. On ouvre la machine, on extrait le disque dur. On fait une première analyse du disque dur sur place, précise un policier. C'est le collègue qui fait l'enquête qui nous dit ce que l'on doit chercher: des images pédophiles, des scanners de fausses monnaies, des courriers électroniques. Quand on "tape" un mec chez lui à 6 heures du matin, on peut rester quatre jours avec le gars en garde à vue. On participe aux auditions car, si le suspect est bon en informatique, il peut noyer l'enquêteur.»

En 2003, l'OCLCTIC a procédé à plus de 200 assistances pour des perquisitions. Quand le ministre est venu, le commandant Philippe a revêtu son uniforme pour faire la leçon: «rechercher un mot dans un disque dur, c'est rechercher un mot dans 65 semi-remorques de papier. En perquisition, on traque les "lacks", les morceaux de fichier non réécrits sur le disque dur. Ça

Libération a suivi durant une semaine le travail de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Les trente-cinq policiers de cet office enquêtent sur toutes les formes de la cybercriminalité (piratages, contrefaçons de cartes bancaires...) et assistent d'autres services dans des affaires de terrorisme, de pédophilie ou de trafics de drogue.



peut être la fin d'une lettre de rançon: "Un ami qui vous veut du bien". Il y a des programmes pour "blanchir" un disque dur, mais un disque "blanchi", ça se voit.» Pour se débarrasser du disque dur, certains emploient parfois les grands moyens. Un jour, Franck montait dans les étages d'un immeuble pour faire une «perquis» alors que le disque dur descendait par le vide-ordures. «Ça nous a pas empêchés de le lire.»

Hervé, flic à la carte

Une carrière de flic, ça tient parfois à un simple bout de plastique de 8 sur 5 centimètres. Hervé, commandant de police judiciaire, est dans la carte bancaire depuis plus de vingt-cinq ans. Il est le griot des moyens de paiement trafiqués à l'OCLCTIC. Il est entré en PJ par l'Office de la

fausse monnaie. Il vous parle d'un temps où, dans la mouvance extrême gauche, on fricotait avec les faux moyens de paiement pour survivre. Hervé a fait ses classes avec les faux traveller's chèques «dans les années 75-76. Ils étaient tellement bien faits que l'Union de banques suisses a suspendu son émission de traveller's chèques durant six mois». «Quand la carte bancaire a commencé, c'était un simple morceau de plastique, raconte Hervé. Petit à petit, on a ajouté des sécurités: les pistes magnétiques, le logo uniquement visible à la lampe à ultraviolet, l'hologramme et la puce.»

Le jeune inspecteur a croisé son premier faussaire de cartes au début des années 80. Avec des cartes vierges et une embosseuse, une sorte de presse à levier qui permet d'imprimer des caractères en re-

lief sur la surface en plastique. «Les gars imitaient de véritables cartes à partir de carbonnes de paiement récupérés dans des poubelles. C'était des proxos, des voyous trop vieux pour monter au braquage qui rentraient dans la combine.» Plus tard, un informaticien a mis au point un skimmer, un petit appareil qui piratait les pistes magnétiques des cartes bancaires. Hervé a croisé ainsi vingt-trois types de cartes contrefaites. Jusqu'à l'arrivée de la puce en 1994. «Ça a tué cette forme de délinquance en France.»

L'officier a gardé dans ses archives des dizaines de rectangles de plastique, grossières copies ou clonages minutieux de cartes bancaires. Il exhibe aussi de drôles d'assemblages sous scellés, mélange compliqué d'électronique et de bricolage maison. «Depuis 2001, beaucoup de pi-

Les désosseurs de disques durs dans le bureau du groupe «assistance technique-interceptions» de l'OCLCTIC à Paris.

ratages de distributeurs de billets sont commis par des gens en provenance des pays de l'Est. Une mini-caméra fixée au-dessus du DAB (3) permet de vous filmer en train de composer votre code secret. Un skimmer placé sur la fente d'introduction du DAB lit vos pistes magnétiques», explique Hervé. Avec ces données, les pirates fabriquent de fausses cartes qui servent uniquement à faire des retraits en Espagne ou en Italie, selon l'officier. «Les malfaçons ne prennent pas de risques. Ils retirent le maximum et n'utilisent que deux ou trois fois la carte piratée.»

JACKY DURAND
photo LIONEL CHARRIER

- (1) Seuls le prénom des policiers apparaît.
- (2) Se taire.
- (3) Distributeur automatique de billets.

(Demain, volet 2: la Triade et ses mules)